Securing the perimeter

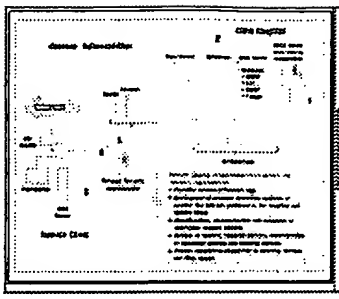
Health Management Technology; Atlanta; Dec 2000; Mark Higgins;

Volume: 21
Issue: 12
Start Page: 8-12
ISSN: 10744770
Subject Terms: Guidelines
Health care industry
Computer networks
Network security
Health Insurance Portability & Accountability Act 1996-US
Classification Codes: **9190**: *United States*
9150: *Guidelines*
5140: *Security management*
5250: *Telecommunications systems & Internet communications*
8320: *Health care industry*
Geographic Names: United States
US

Abstract:
*Faced with challenges such as increasing **cost** pressures, a need to integrate legacy information systems, and federal regulations that encourage the use of electronic transactions, many **healthcare** organizations have initiated large-scale deployments of Internet technologies and introduced a host of remote access capabilities. Follow a step-by-step process to **optimize** the security of remote access points and to demonstrate Health **Insurance** Portability and Accountability Act (HIPAA) compliance. Health care IT administrators may choose to outsource several or all of these steps to a third party specializing in **network** security: 1. Create a **network** diagram. 2. Identify common vulnerabilities. 3. Review HIPAA requirements. 4. Eliminate vulnerabilities. 5. Monitor and re-evaluate.*

Full Text:

[Headnote]
Strategies to secure remote access points to healthcare IT networks.



Enlarge 200%
Enlarge 400%

Faced with challenges such as increasing cost pressures, a need to integrate legacy information systems, and federal regulations that encourage the use of electronic transactions, many healthcare organizations have initiated large-scale deployments of Internet technologies and introduced a host of remote access capabilities.

While the use of Internet technologies offers many benefits, information technology (IT) administrators cannot ignore the corresponding security risks. Simply stated, when healthcare organizations allow individuals to access network resources remotely, the risk of a security breach increases exponentially.

The Health Insurance Portability and Accountability Act (HIPAA) Security and Electronic Signature Standard present IT administrators with added pressure to secure their networks. Once the final rule becomes enforceable (expected in early 2003), the establishment of stringent security policies will no longer be optional-federal law will require them. In the wake of these developments, there are specific security vulnerabilities and federal requirements to be considered when and if healthcare IT administrators allow remote access to the network.

Backdoor Dial-up Points. Unrestricted dial-up points enable unauthorized individuals to bypass the firewall and gain direct access to the server using the dial-up connection. In the example above, the UNIX server can be accessed using this strategy.

Use of Unnecessary Services. Telnet services may be accessible on a server despite the fact that the server is only used for WWW and FTP services. This practice increases the number of potential entry points for unauthorized entities at no added benefit to the healthcare organization. The Web server offers Telnet and MAIL even though WWW and FTP are the only services required by users.

Poor (or Non-Existent) Access Controls. The remote clinic has not deployed a firewall to guard against unauthorized access through the DSL connection to the remote clinic. If configured correctly, the firewall would only allow HTTP and FrP though the firewall; all other packets would be dropped.

Insufficient Auditing/Monitoring. The network security administrator fails to conduct periodic reviews of firewall logs and has not deployed an intrusion detection system. Unfortunately, even if the administrator did perform periodic reviews, this strategy is almost equally ineffective. Hackers can attack the network at any time; therefore, periodically reviewing logs fails to prevent most attacks. This strategy simply identifies security breaches after they occur.

Weak Configuration Management. The network security administrator failed to install a patch to the Web server, allowing hackers to exploit the vulnerability and compromise the server.

Step-by-Step Security

Follow a step-by-step process to optimize the security of remote access points and to demonstrate HIPAA compliance. Healthcare IT administrators may choose to outsource several or all of these steps to a third party specializing in network security.

Step 1:

Create a Network Diagram.

Start with an accurate diagram outlining all of the network resources in place. Consider:

* Physical and logical barriers for all mainframes, servers, workstations

* Location of remote access points (e.g., Internet gateways, dial-up points)

* Number of remote users and remote locations

Step 2:

Identify Common Vulnerabilities.

These vulnerabilities should be placed on the network diagram. Consider:

* Are dial-up points behind the firewall protected with strong authentication?

* Are non-essential services on servers disengaged?

* Are Internet gateways protected by firewalls?

* Are security devices routinely patched?

* Should this function be outsourced to an organization specializing in network security?

Step 3:

Review HIPAA Requirements.

Evaluate each remote access point on the network diagram and determine which technologies and/or processes need to be in place to ensure compliance with HIPAA.

* Is the Internet gateway protected with authentication and firewalls?

* Are there intrusion detection systems to monitor traffic through remote access points?

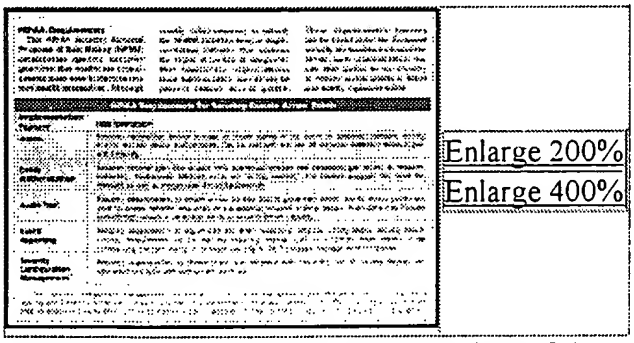
* Do information security personnel identify new vulnerabilities and install patches to security devices immediately upon release to the public?

* Do information security personnel frequently review firewall logs, intrusion detection alerts, and other data sources to identify potential security breaches?

* Do information security personnel document instances of suspicious activity and/or security device malfunctions?

Step 4:

Eliminate Vulnerabilities.



HIPAA Requirements for Securing Remote Access Points

Revise policies and/or identify technologies and services that address the vulnerabilities and instances of noncompliance with the HIPAA security requirements.

* Do I have the expertise to fix these vulnerabilities or should I outsource to network security experts?

* If new technologies ar necessary, what are the cost/benefits of different products and services on the market?

Step 5: Monitor and Re-evaluate. Technologies and processes that should be in place to ensure continued compliance include:

* Intrusion detection systems. These systems automate the alarm generation function in the event of suspicious network activity. They are helpful (and necessary) to automate the monitoring of traffic passing through the Internet gateway.

* Constant security monitoring and management. Outsourced security monitoring and maintenance services detect and respond to suspicious network activity in real-time, as well as ensuring that all security devices are configured correctly and patched promptly. This capability allows organizations to comply with the alarm, entity authentication, audit trail, event reporting, and security configuration management requirements under the HIPAA Security NPRM.

* Periodic network security assessments. Conduct a comprehensive assessment of the network security posture at least annually, with either internal or outsourced resources.

[Author note]
Mark Higgins is director of healthcare strategy at RIPTech Secure Solutions, Alexandria, VA. He can be reached at mhiggins@riptech. com.
